

スパイウェアの現状等について

平成18年2月21日
総務省情報通信政策局総合政策課

最近の主なスパイウェア関連事件

01年12月	ネットカフェに仕掛けたキーロガーでパスワードと盗用、被害額270万円の容疑者逮捕	05年7月	全国銀行協会はスパイウェアによる一連の不正出金被害は合計940万円と発表
03年3月	シティバンクの顧客口座から1600万円を不正出金した容疑者男性2人を逮捕	05年10月	米ソニーBMG社の音楽CDに情報を送信するツールが発見される
04年6月	都内の2カ所のネットカフェに仕掛けたキーロガーでオークションIDが盗難、被害額196万円	05年11月	千葉銀行はスパイウェア混入のCD-ROMが顧客3件に郵送され1件で不正出金されたことを発表
04年10月	キーロガーによる不正アクセス禁止法違反と電子計算機使用詐欺の疑いで男性1人逮捕	05年11月	北陸銀行はスパイウェア混入のCD-ROMが顧客1件に郵送され不正出金未遂があったことを発表
05年3月	三井住友銀行ロンドン事務所からハードウェアを用いた約451億円の不正出金未遂が判明	05年11月	ジャパンネット銀行、千葉銀行など預金詐欺容疑者2人逮捕、被害額は10口座1140万円
05年7月	イーバンク銀行は顧客口座1件から13万円を不正出金されたことを発表	05年11月	米ソニーBMG社は問題の音楽CDの製造を中止することを発表
05年7月	みずほ銀行は顧客口座2件から不正出金されたことを発表、被害額は未公表	05年11月	米ソニーBMG社は問題の音楽CDを店頭から回収し無料交換することを発表
05年7月	ジャパンネット銀行が顧客口座6件から379万円を不正出金されたことを発表		

ソニーBMGが採用している違法コピー防止ソフトを巡る動き

- ソニーBMGが販売する音楽CDの一部に採用された違法コピー防止ソフト「XCP DRMソフトウェア」に、悪質なソフトウェアに分類される“rootkit”と呼ばれるプログラミング技術が使われていることが判明。
- ユーザがパソコンに音楽CDを挿入し、使用許諾契約に同意すると、XCPと専用の音楽CD再生ソフトウェアがパソコンにインストールされる。これにより、著作権保護機能付きの音楽ファイル(WMA形式およびATRAC形式)をパソコンに取り込めるほか、バックアップ用のディスクを作成できるようになる。
- XCPの問題視された点は、①ユーザが認知できない状態でPCにインストールされる点、②一度インストールすると容易には削除できない点、及び③XCPがインストールされたPCには、ごく基本的なアクセス権さえ入手できれば、どんなファイルでも不可視にすることができる点などである。

ソニーBMGの音楽CDに関連する一連の出来事

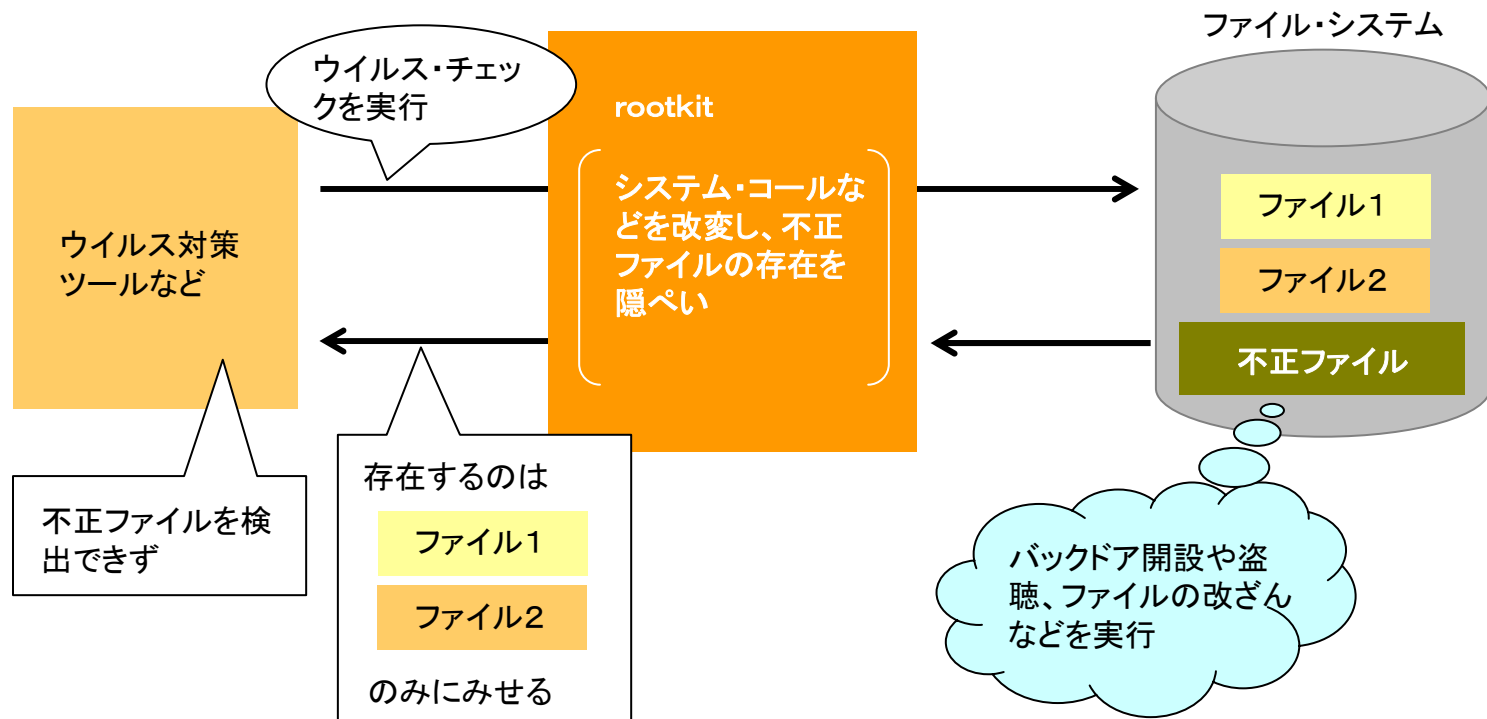
日付	出来事
11月1日	フィンランドF-Secureなどが、ソニーBMGの音楽CDに含まれるコピー防止ソフト「XCP」が“rootkit”の機能を使っていることを指摘
11月2日	“rootkit”の機能を無効にするサービス・パックやXCPのアンインストール・ツールの提供開始
11月8日	サービス・パックのアップデート版を公開
11月10日	XCPを含む音楽CDの製造を一時中止。XCPを悪用するウイルス(悪質なソフトウェア)が出現
11月12日	米MicrosoftなどがXCPの一部をウイルスとみなし、対応を表明
11月15日	XCPのアンインストール・ツールに問題発覚。配布を一時中止
11月16日	アンインストール・ツールを悪用するサイトが出現
11月18日	XCPを含む音楽CDの交換および回収を開始
11月21日	日本国内の輸入元がXCP入り音楽CDの交換および回収を開始

rootkit(ルートキット)とは？

- “rootkit(ルートキット)” は、一度侵入したシステムに対して、その後システムを悪用しやすいように改変するためのツール群の総称で、特に悪質で気付かれにくいトロイの木馬の一種。
- ルートキットは、オペレーティング・システム(OS)の最も基本的なレベルを改変して、ユーザーやプログラムがその存在を検知できないようにする。通常の悪意あるコードならファイル名を偽装する程度だが、ルートキットは、自らの存在を明かすようなOSの通信を「横取り」し、虚偽の情報を伝えるようプログラムし直してしまう。

出所) NIKKEI Electronics 2005.12.19, Hotwired Japan 2005.11.2 など

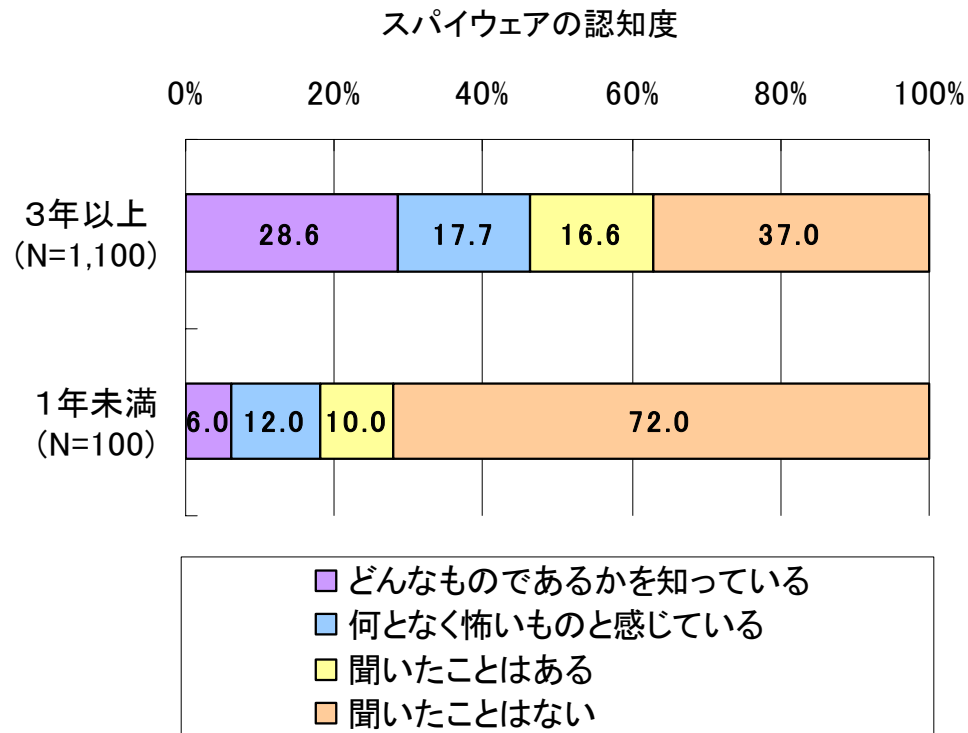
rootkitが隠した不正ファイルの存在はウイルス対策ツールも発見できない



出所) NIKKEI COMPUTER 2005.11.28

スパイウェアの認知度

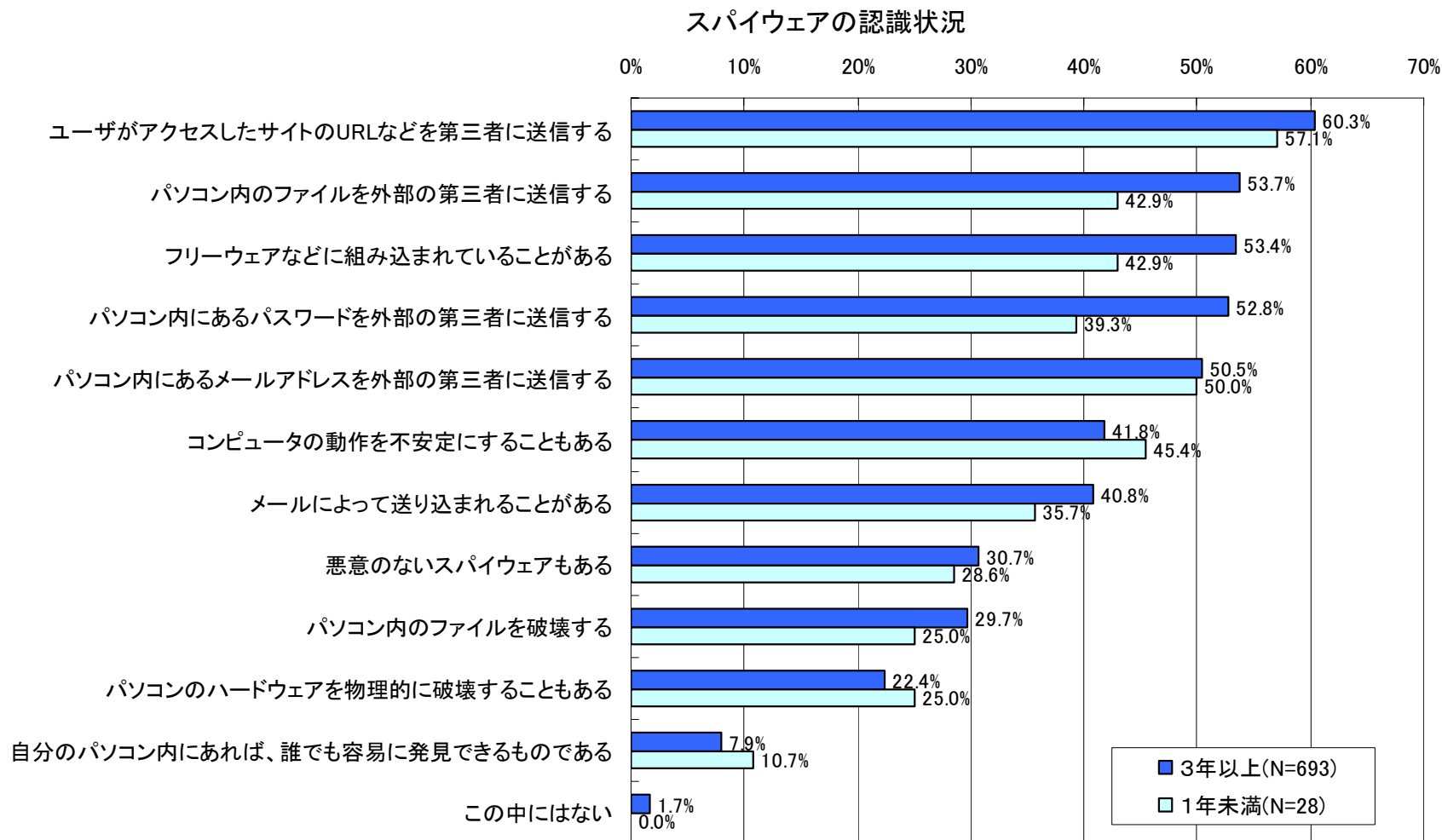
- ネット歴3年以上の利用者層においても、スパイウェアを認知している割合は3割にも満たない状況。
 - ネット歴1年未満の利用者層では、さらに認知率が低下し、6%にとどまっている。



出所)シマンテック(2005年1月中旬に調査)

スパイウェアの認識状況

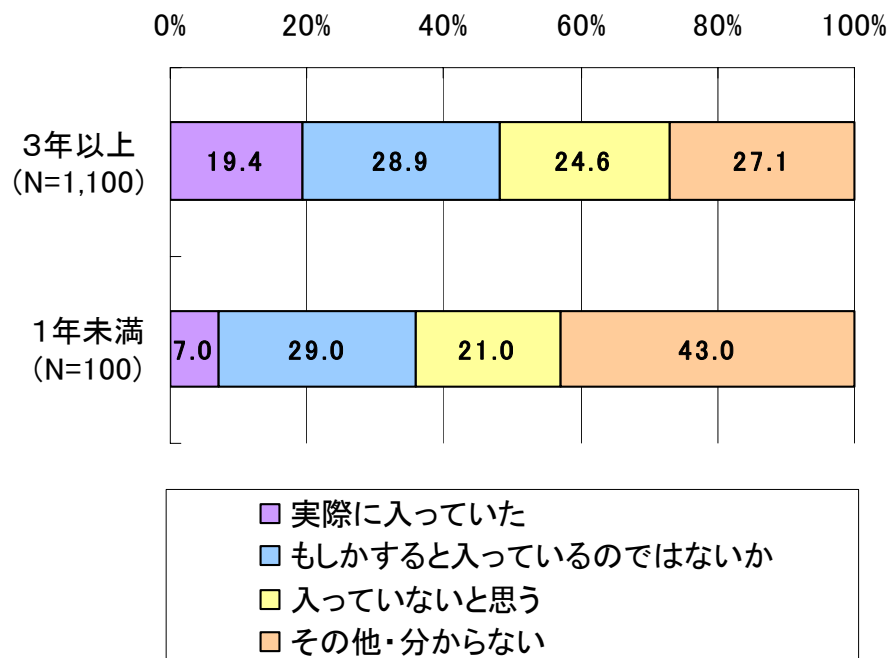
- ユーザからみたスパイウェアのイメージは、アクセスサイトのURLやパソコン内のファイル、パスワード、メールアドレスを外部の第三者に送信するもの。



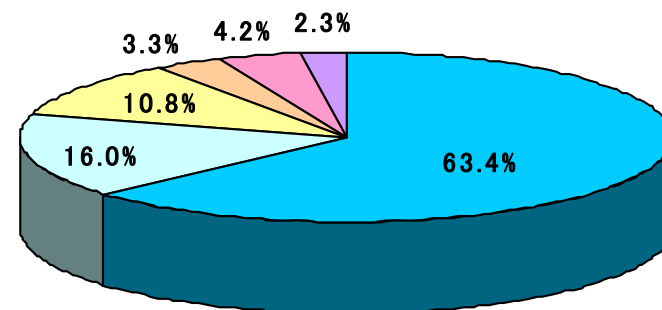
スパイウェアの侵入可能性・発見された スパイウェアの内容

- ネット歴3年以上の利用者層の約2割がスパイウェアの侵入を経験。
 - また、「もしかすると入っているのではないか」と不安視している者も約3割。
 - スパイウェアの発見種類は、「1～10種類」が最多。また、31種類以上発見した者も約1割に及ぶ。

スパイウェアの侵入可能性



発見されたスパイウェアの種類



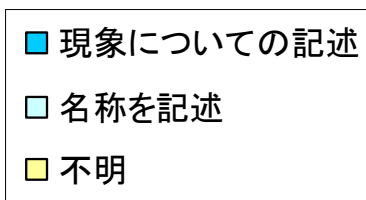
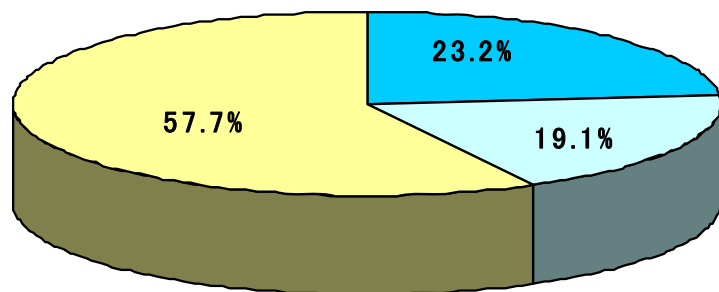
- 1～10種類
- 11～20種類
- 21～30種類
- 31～40種類
- 41～50種類
- 51種類以上

※ネット歴3年以上で実際にスパイウェアが入っていた人を対象

発見されたスパイウェアの内容

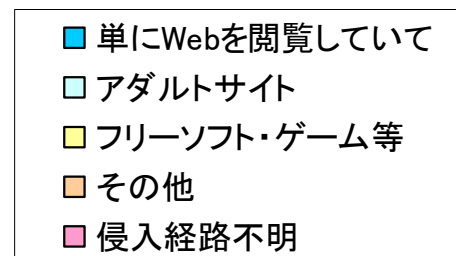
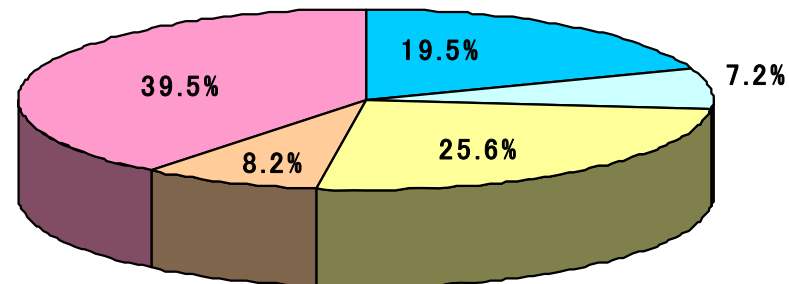
- スパイウェアの侵入をソフト等により発見した者のうち、約6割はそのスパイウェアの具体的機能や名称を知らない。
 - 侵入経路の心当たりとしては、「フリーソフト・ゲーム等」、「単にWebを閲覧している」が上位を占める。

スパイウェアの内容



※有効回答220例を対象

スパイウェアの侵入経路の心当たり

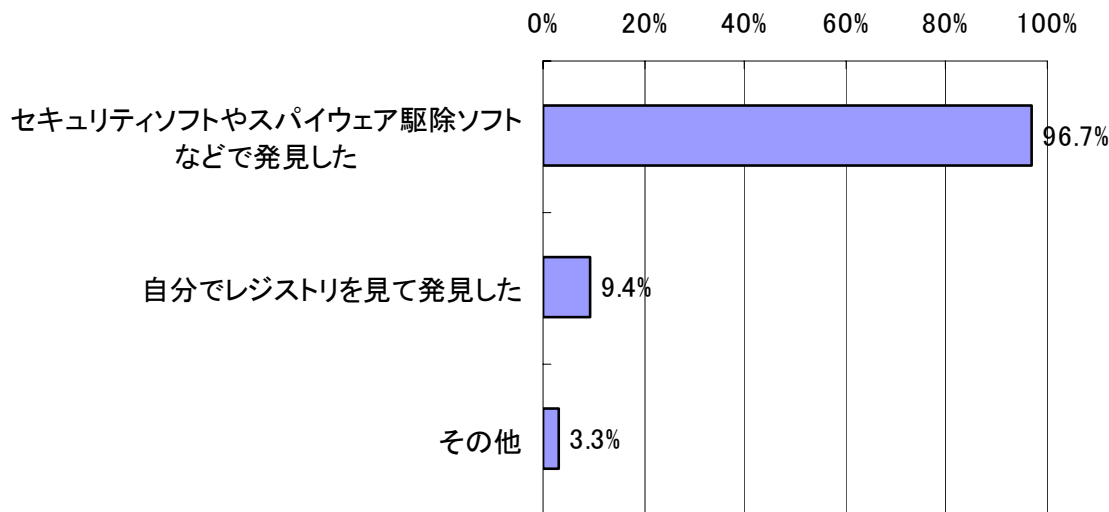


※有効回答195例を対象

スパイウェアの発見方法

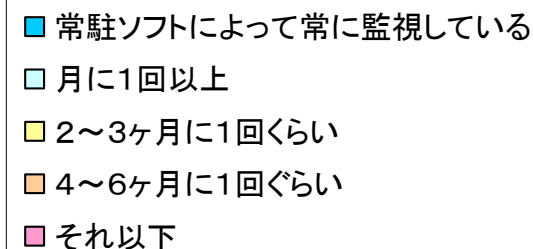
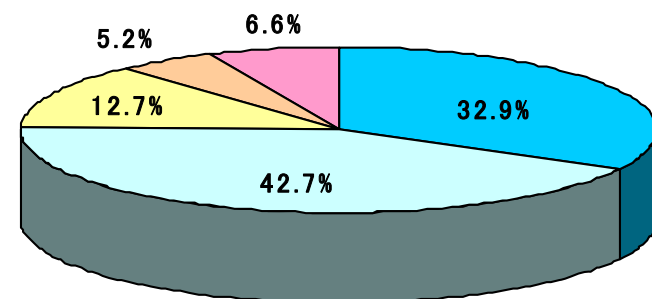
- セキュリティソフトやスパイウェア駆除ソフトなどでスパイウェアを発見するケースがほとんど。
 - チェック頻度は、「月に1回以上」が最多。常駐ソフトによって常に監視している者も3割を上回る。

スパイウェアの発見方法



※ネット歴3年以上で実際にスパイウェアが入っていた人を対象

スパイウェアのチェック頻度

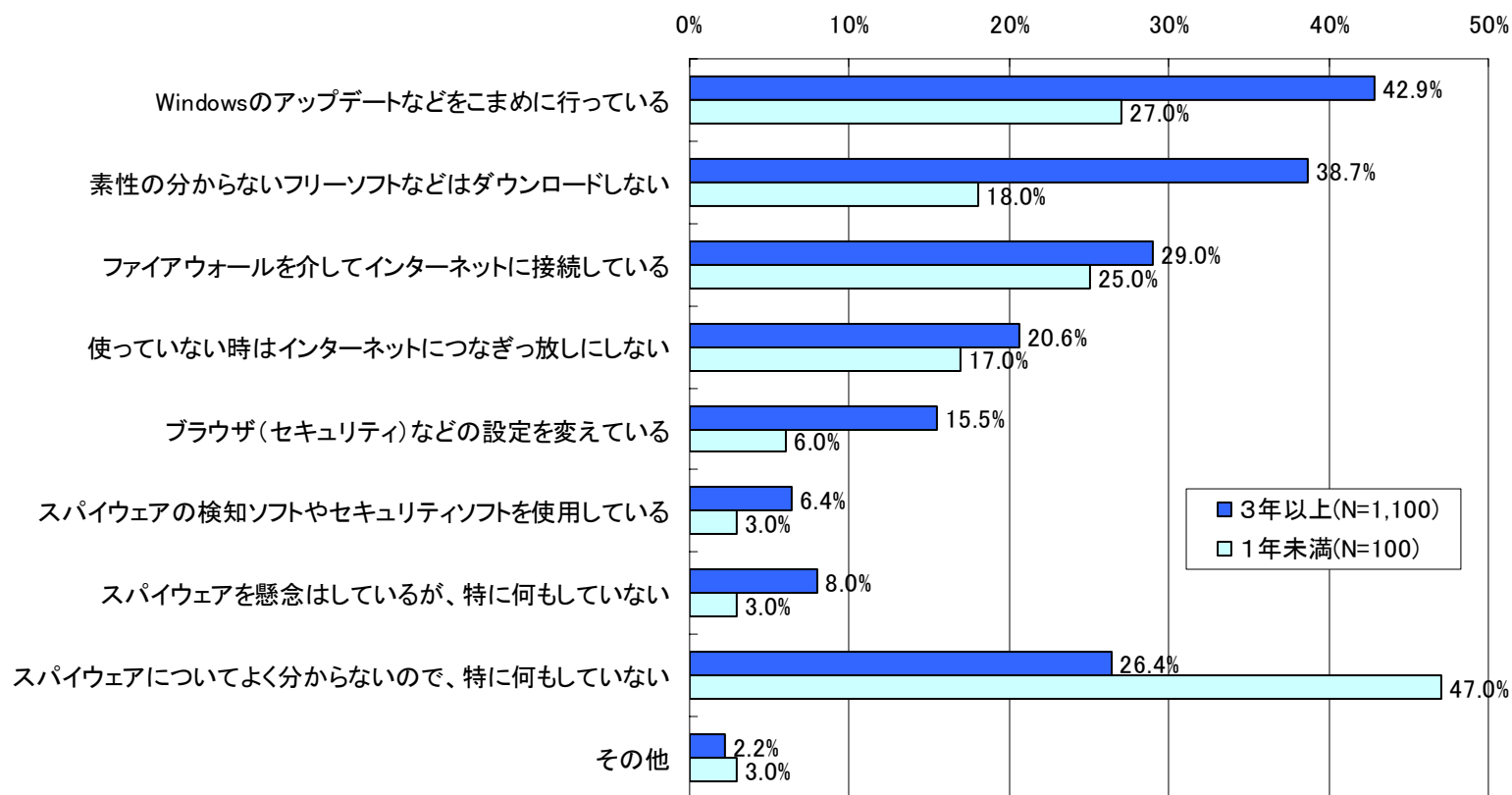


※ネット歴3年以上で実際にスパイウェアが入っていた人を対象

スパイウェア対策

- ネット歴3年以上の利用者層においても、26.4%が「スパイウェアについてよく分からないので、特に何もしていない」、8.0%が「スパイウェアを懸念はしているが、特に何もしていない」と回答。
 - ネット歴1年未満の利用者層では、半数近くが「スパイウェアについてよく分からないので、特に何もしていない」と回答。

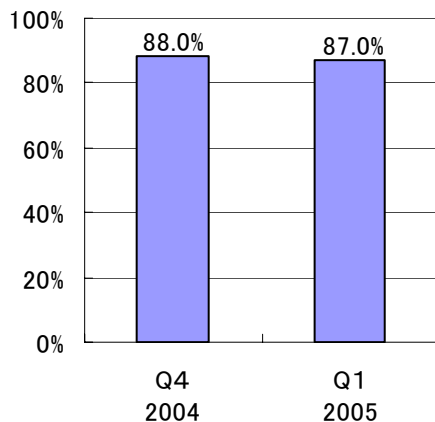
スパイウェア対策



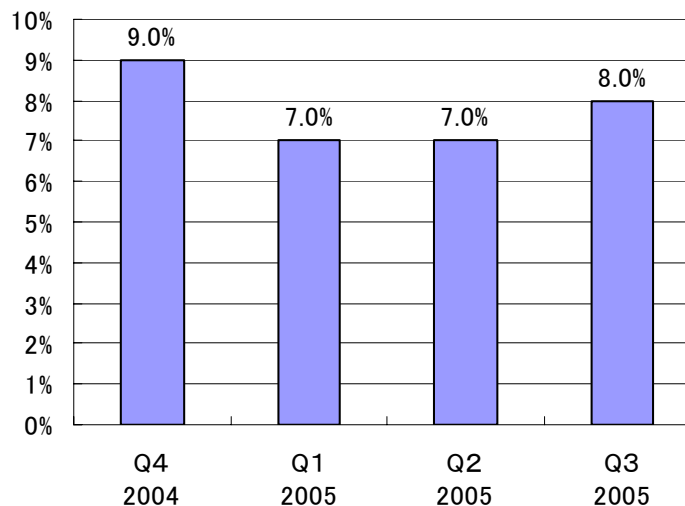
海外におけるスパイウェアの現状

- 企業内のパソコンの8%が悪意あるスパイウェアに侵入を経験。
 - また、企業内のパソコンの87%が悪意のないものも含め何らかのスパイウェアの侵入を経験。パソコン1台当たり平均27個のスパイウェアが発見されている。

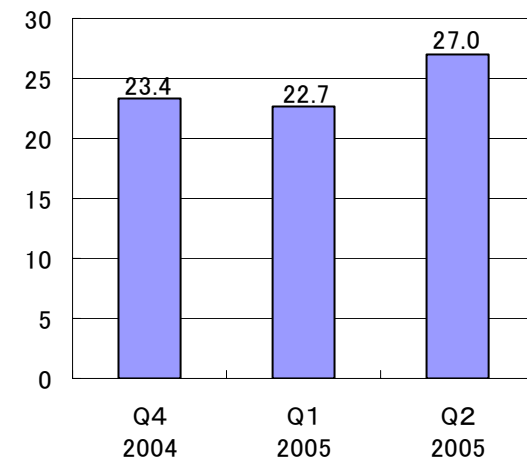
Instances of Spyware
Percent of Machines with Instances of Spyware
in the Enterprise



Instances of Malicious Spyware
Percent of Scans with Instances of Spyware in the Enterprise



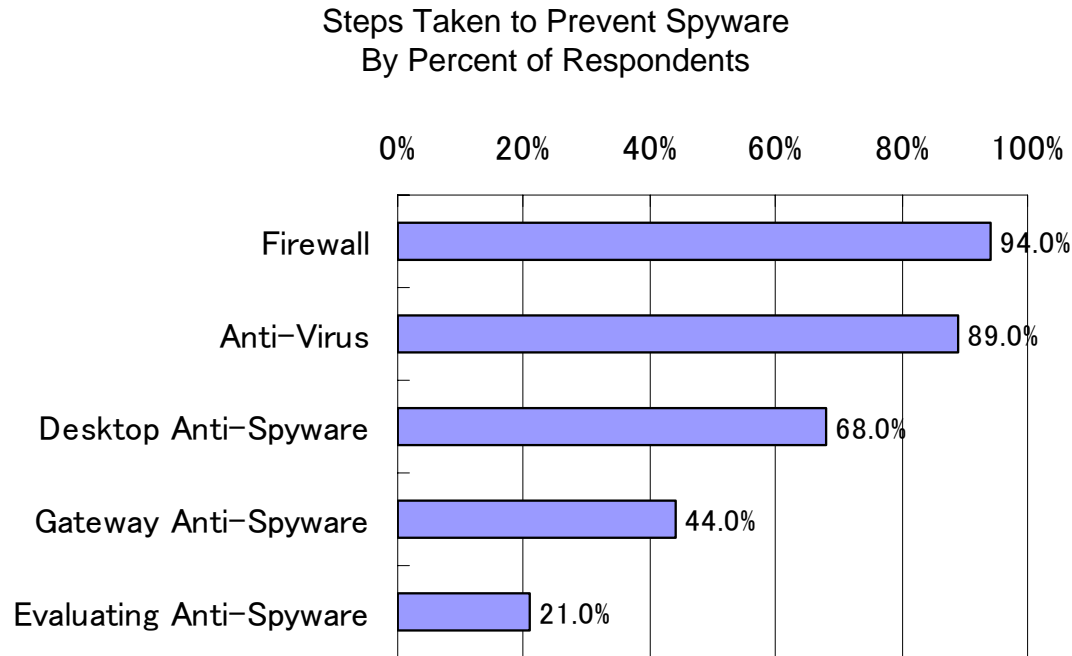
Instances of Spyware
Average Instances of Spyware per Infected PC



※System Monitors, Trojan Horsesが対象

海外におけるスパイウェア対策

- スパイウェア対策としては、ファイヤーウォールの設置が94%、ウィルス対策ソフトの導入が89%、デスクトップのPCにスパイウェア対策ソフトを導入している割合が68%となっている。

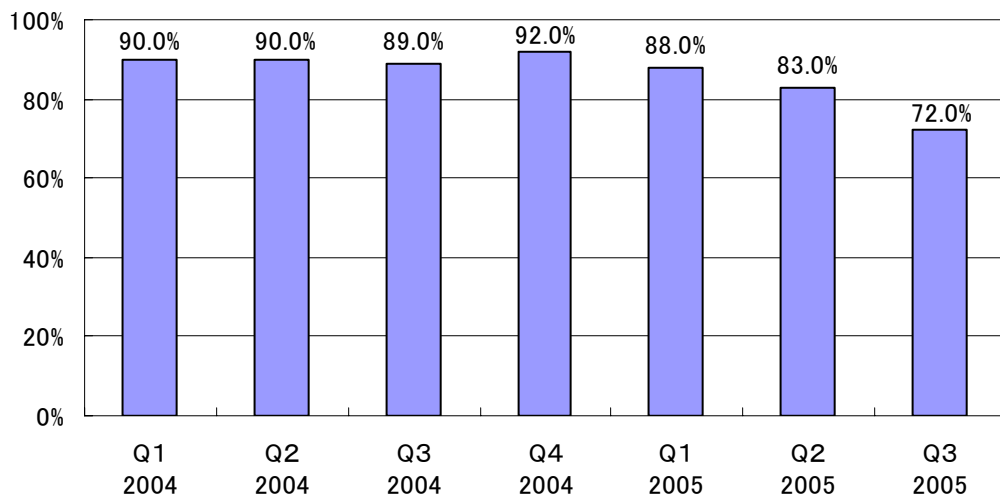


出所)「STATE OF SPYWARE」(Webroot社)

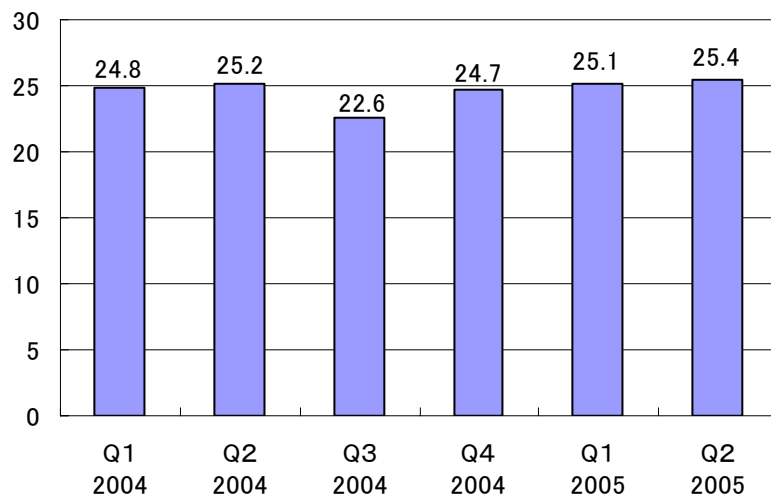
海外におけるスパイウェアの現状

- 家庭内のパソコンの72%が何らかのスパイウェアの侵入を経験している。
 - 1スキャン当たり平均25個のスパイウェアが発見されている。

Instances of Spyware
Percent of Scans with Instances of Spyware in the Consumer Market



Instances of Spyware
Average Instances of Spyware per Scan



※System Monitors,Trojan Horses,Adware,Tracking Cookiesが対象